Some challenges in wireless security

Suman Banerjee
Department of Computer Sciences, University of Wisconsin, Madison, WI 53706, USA
Email: suman@cs.wisc.edu

1 Introduction

Wireless communication technologies provide users with significant flexibility and portability and hence is being widely adopted as a preferred mode of communication in many military and civilian applications. By eliminating the need for devices to be tethered by wires, such technologies enable new usage scenarios not otherwise possible. A number of mobile, in-range wireless devices can self-organize themselves into an ad-hoc network — such capabilities have many applications, e.g., for first responders.

However, such increased flexibility comes with increased vulnerabilities. Many unique vulnerabilities in the wireless environment occur due to the shared and open nature of communication. In this short document, we discuss some of these new threats, recent approaches to mitigate them, and further challenges that need to be addressed.

2 Potential threats

While many of the vulnerabilities in wireless environments are similar to those in a wired network, others are fairly unique in nature. A lot of ongoing research and design efforts are addressing many of these vulnerabilities. Some of these issues that have received significant attention in recent years include mutual authentication to users prior to communication, as well as data confidentiality, and data integrity. For example, the 802.11i standards are being used to provide such authentication in wireless LAN environments [1]. However, even if these concerns are reasonably addressed, many further challenging security concerns remain.

- Availability attacks: The goal of these attacks are to reduce the availability of the wireless medium to legitimate users. The inherent broadcast nature of the wireless medium implies that an attacker can easily mount such attacks by selectively interfering with legitimate communication. For example, an attacker can transmit packets with high NAV values, that prevent any legitimate user from accessing the channel for long durations of time.

- Energy attacks: An attacker can easily send wireless traffic to a victim node that requires the latter to process such traffic prior to realizing such traffic to have no local relevance. However, the effort of decoding such traffic requires power consumption, and slowly drains the battery of the mobile node. Such attacks are easy to mount and require sophisticated strategies to combat.

- Location privacy and authentication: An attacker can monitor communication patterns in the medium to continuously track the location of different users in the environment. In order to guard against such attack capabilities, it is important to design strategies that allow users privacy of their location information. However, design of such tools can benefit attackers too — if location privacy can be carefully preserved, then attackers can utilize them to hide their own location from the system.

3 Approaches to mitigate such attacks

We now discuss some approaches that may be useful in mitigating such attacks in wireless environments.

- Availability attacks: The simplest form of an availability attack is PHY layer 'bit-jamming' approach, where the attacker causes continuous interference on the medium. Such attacks, however, are energy inefficient. They require attackers to expend a lot of energy, a process which can potentially make the attack

detection and mitigation tasks easier. In contrast, an intelligent attacker may choose to attack the MAC layer of the protocol stack. Since MAC layers typically define cooperation-based techniques for medium access, an attacker (a non-cooperating node) can selectively mount attacks on specific MAC control frames to disrupt all MAC level communication. Such an attack incurs very low energy costs at the attacker.

Hence, mitigation of availability attacks both at PHY and MAC layers should be an important component of the wireless security research agenda. At the PHY layer, number of interesting approaches can be researched, including various channel-matched signaling schemes, efficient packet coding, on top of conventional spread-spectrum and antenna nulling approaches. At the MAC layer, it may be possible to design new MAC protocols that utilize randomization and obfuscation techniques making it difficult for attackers to opportunistically attack or fake MAC control frames.

- Energy attacks: These attacks are quite simple to mount and yet very effective in disrupting communication. Within the context of this workshop, these attacks are are applicable to both MANETs and mobile phones. For mobile phones this problem can be particularly vexing, since the user has no explicit way of pre-filtering against such irrelevant messages sent by an attacker. We believe that proper security against these attacks would be multi-dimensional. One component of the solution will include support from less energy constrained devices that are not necessarily co-located with the device under attack. Another approach may be to design strategies that can quickly evaluate the value of incoming packets to the user. However, the speed (and energy costs) of such evaluation would trade-off against the accuracy of the decision process.

- Location privacy and authentication: There is an inherent tradeoff between the privacy of location information of users and the ability for the system to authenticate the same information. The biggest challenge in maintaining location privacy stems from the ability of an attacker to triangulate the location of a transmitter based on received signal strength, angle or arrival, and other such properties. Different strategies can be considered to provide location privacy both at PHY and MAC layers. For example, it might be possible to utilize antenna-nulling techniques that obfuscate signal strength information. Similarly, the system may design techniques to induce additional interference that achieves the same effect.

Location authentication is also a difficult problem because tools useful for privacy can be employed by attackers to guard against the system's ability to determine the user's or the attacker's location. Past research has studied different statistical techniques for location determination that are based on received signal strength from different transmitters at a given location. However, location determination based on received signal strength information is relatively easy to attack. In particular, an attacker can construct efficient models that allows it to infer received signal strength in different parts of the physical space. Such a capability will allow an attacker to fake its own location to the system. Some recent work utilizes the notion of wireless congruity [2], which provides location authentication based on the "common experience" of nodes that are physically close to each other. Hence, if the location of a set of trusted reference points can be determined, then a proximity metric can be defined that allows for location authentication. Further evaluation of these and other such schemes need to studied.

Finally, the tradeoffs between location privacy mechanisms and the need for location authentication is a challenging domain of work and will be an important direction of future study.

References

[1] IEEE. Amendment to standard for telecommunications and information exchange between systems - LAN/MAN specific requirements - part 11: Wireless medium access control (MAC) and physical layer (PHY) specifications: Medium access control (MAC) security enhancements. IEEE Standard 802.11i, 2004.

[2] A. Mishra, S. Rayanchu, A. Shukla, and S. Banerjee. Towards robust localization using wireless congruity. In *ACM HotMobile*, February 2007.

Adversary models in wireless security

Suman Banerjee
Department of Computer Sciences
suman@cs.wisc.edu

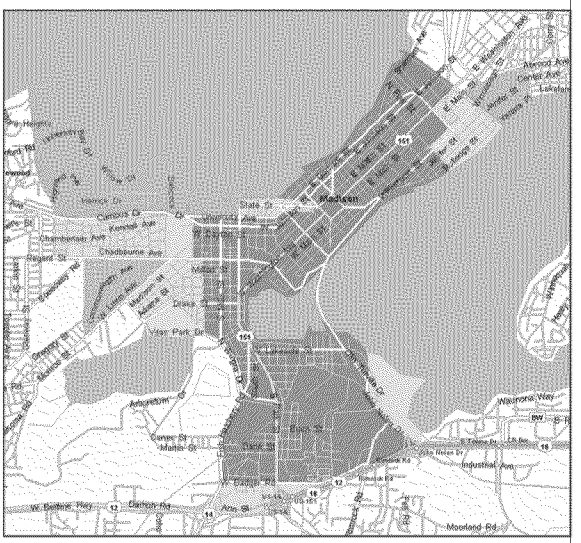
Wisconsin Wireless and NetworkinG Systems (WiNGS) Laboratory

Wireless localization

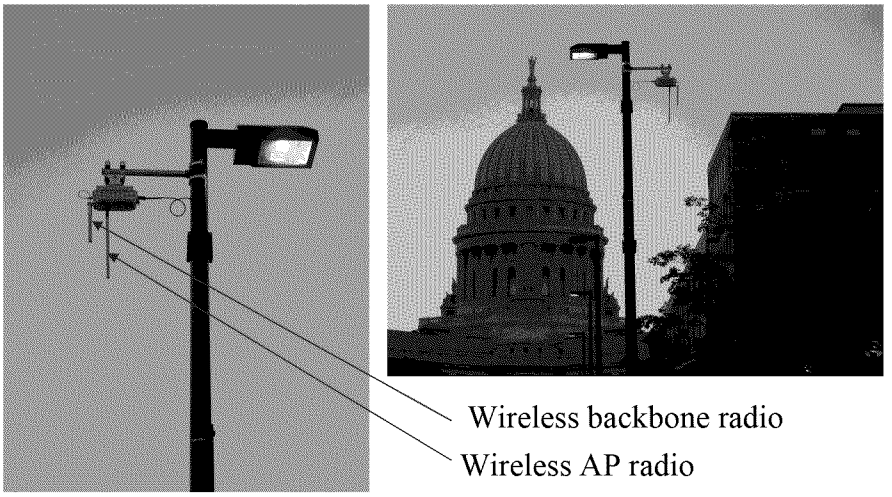
Madison municipal WiFi mesh network

•

• 9 square miles area
• 200+ APs

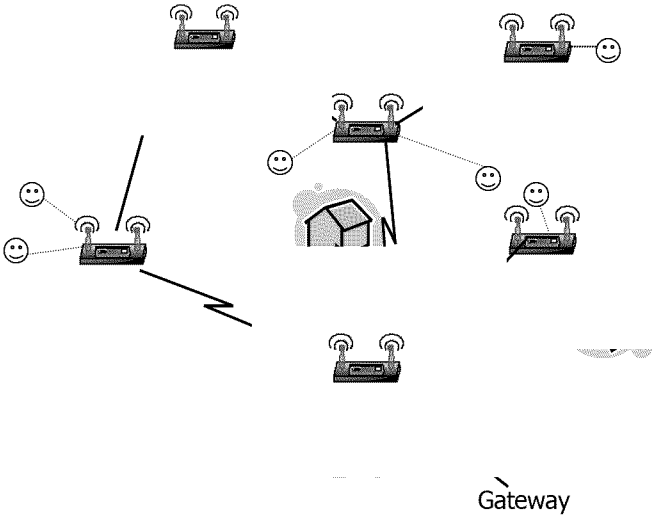


Municipal Wi-Fi Mesh in Madison



Mesh AP on street light

Municipal Wi-Fi Mesh in Madison

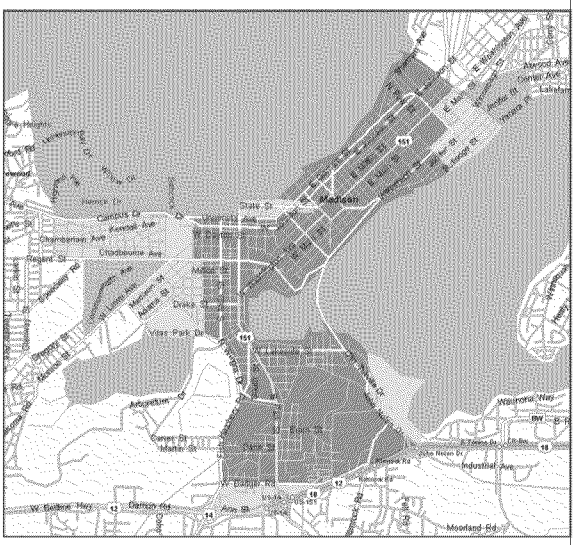


Location applications

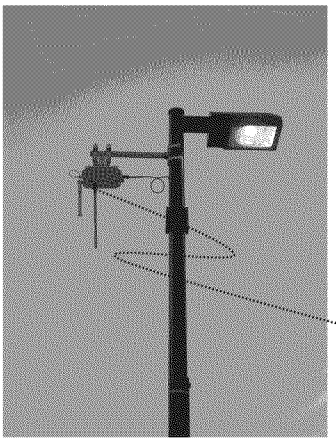
•Assume a disaster scenario

Locate position of each rescue personnel within the city in a reliable, secure fashion

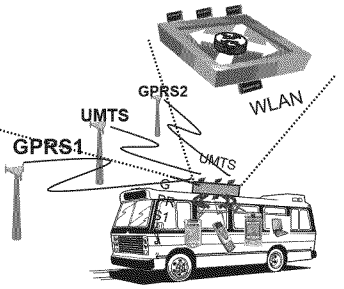
Can take advantage of existing (trusted?) WiFi mesh deployment and wireless communication of rescue personnel



Location applications



- Real-time city-bus fleet management
- Where are the different buses?

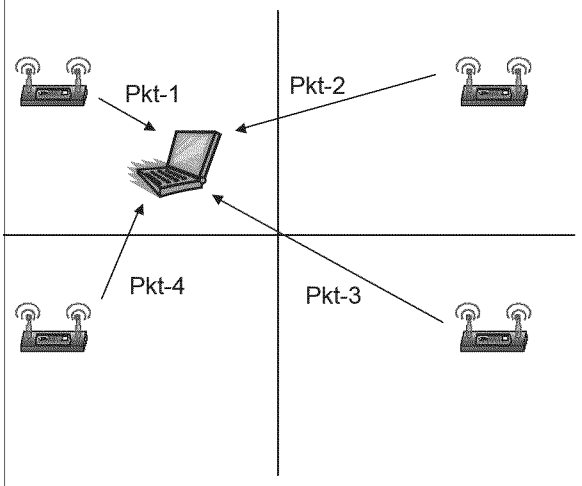


Location security

- Prove a user's location to the infrastructure
- GPS does not help

- Adversarial scenarios:
  - Integrity attacks:
    - Attacker pretends to be in a different location
    - Attacker makes the system believe that the victim is in a different location
  - Privacy attack:
    - Attacker infers location of victim and can track the victim

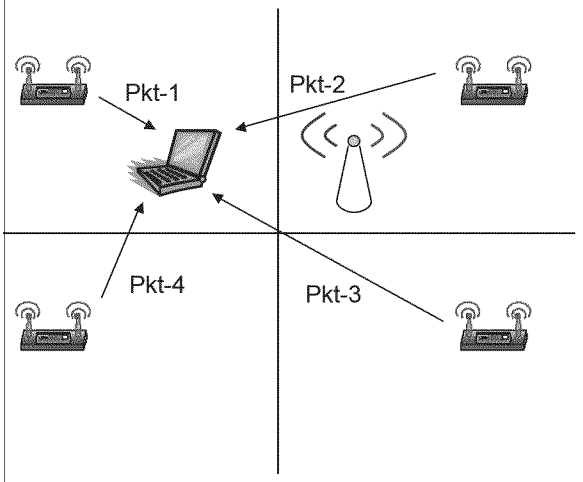
A specific localization approach



- Partition space into a grid
- System transmits some packets
- Participant reports RSSI tuple observed

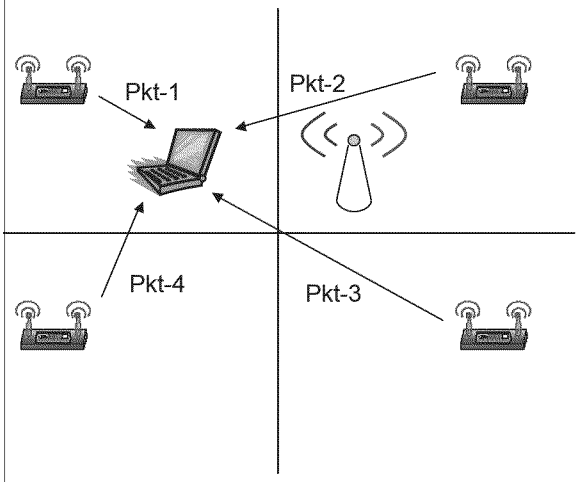
- RSSI tuple is unique to a location and is the location signature

Adversarial models (1)



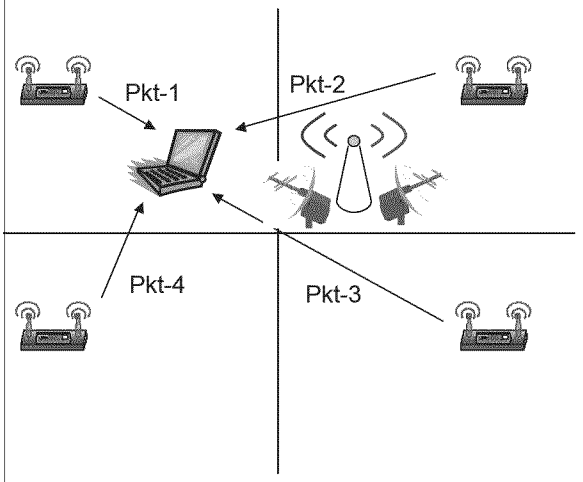
- Attacker present in one location and observes all traffic using a regular antenna
  - May be able to infer the RSSI tuple at victim

Potential countermeasure



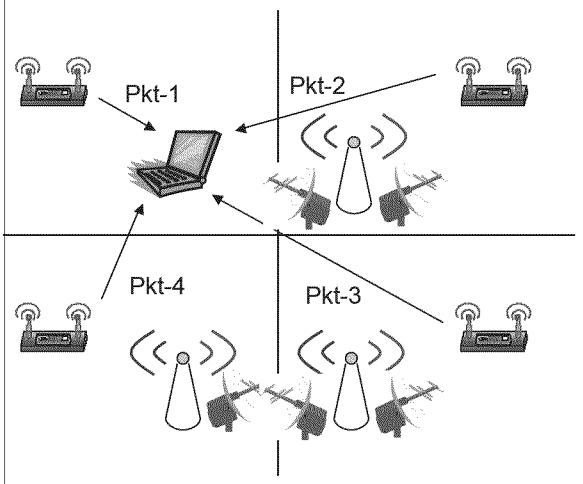
- System can employ randomization
  - Hide transmitter MAC address
  - Use random transmit power each time
- Attacker may not know which packet is transmitted by which transmitter
  - Makes inferencing difficult

Adversarial models (2)



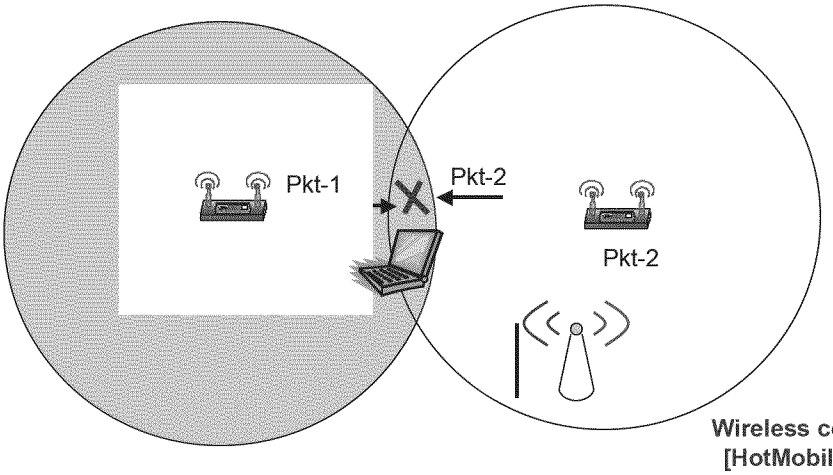
- Attacker able to tell Angle/Direction-of-Arrival
- Randomization may not help

Adversarial models (3)



- Even more sophisticated attacker
  - Present in multiple locations
  - Can allow attacker to have better location inference

More countermeasures



Wireless congruity
[HotMobile 2007]

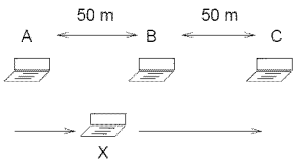
Time-scheduled transmissions by the system that induce collisions may make inferencing harder

Wireless "congruity"

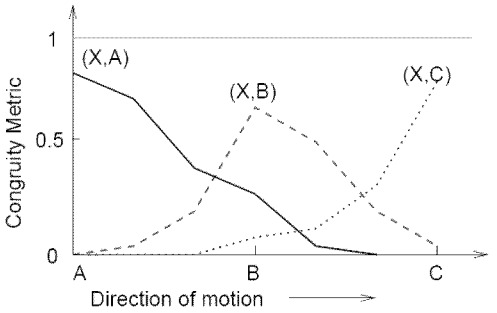
- Very robust in environments with high *entropy*
- First metric : $\zeta(A,B) = \frac{N_{AB}}{N_A + N_B - N_{AB}}$

- A is a trusted monitor, B is the user being authenticated

Congruity implies spatial vicinity



(a) Topology A

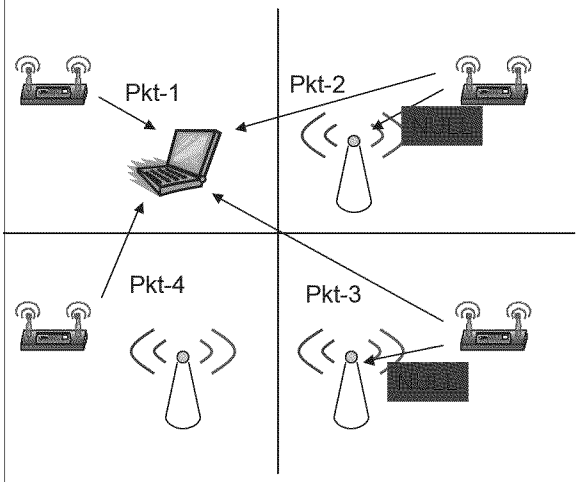


Based on the "congruity", it is possible to say if X is near A, B or C

Optimizations

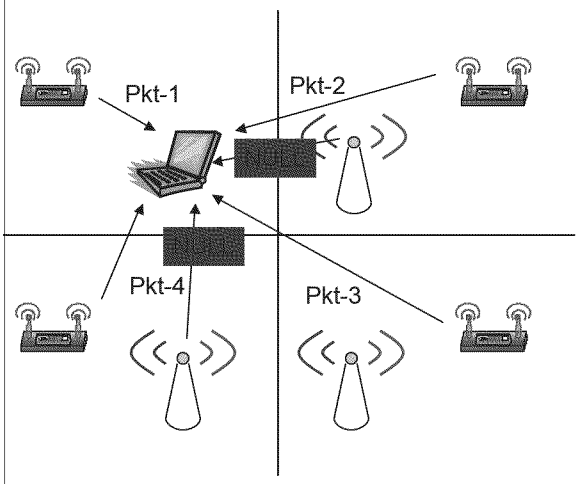
- Considering packets in *error* is useful
- Thresholding on RSSI of correctly received packets can also be useful
- Summary:
  - Wireless congruity is a promising approach to implement robust location authentication

More countermeasures



- Trusted system can use MIMO to create NULLs in certain directions
- Not always easy to determine directions to NULL
- Has other pitfalls

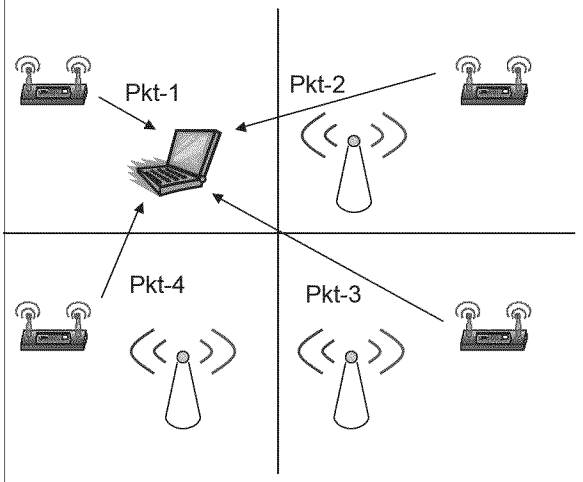
Adversarial models (4)



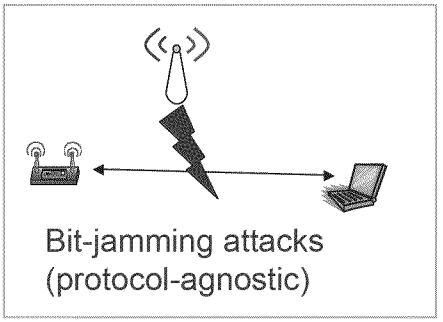
- Adversary can create NULLs at the victim as well

Adversarial models (5)

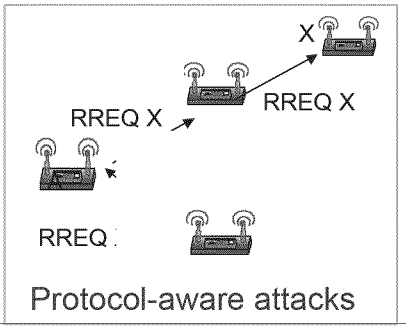
- Captured node in the system



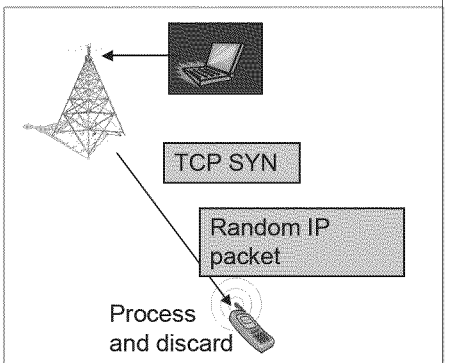
More adversarial scenarios



Bit-jamming attacks
(protocol-agnostic)



Protocol-aware attacks



Behavioral attacks

Range of adversary capabilities

- Protocol knowledge
- Energy source
- Location diversity (what communication can it observe and affect)
- PHY layer capabilities – MIMO, AoA/DoA inference, antenna sensitivity, wormholes
- Computation capability
- Characteristics of the wireless topology itself

- Malice vs mal-function/selfish
- Collusions
- Tradeoff against performance, resilience, and other metrics

Summary

- Most popular wireless communication mechanisms are relatively easy to attack
- Adversarial models not carefully considered when these protocols were designed

Thank you!

Suman Banerjee

Email: suman@cs.wisc.edu

Department of Computer Sciences
University of Wisconsin-Madison

http://www.cs.wisc.edu/~suman

Wisconsin Wireless and NetworkinG Systems (WiNGS) Laboratory